One Step Ahead

An Insight into Performing Rapid Incident Response

Mike Scutt and Shanna Battaglia

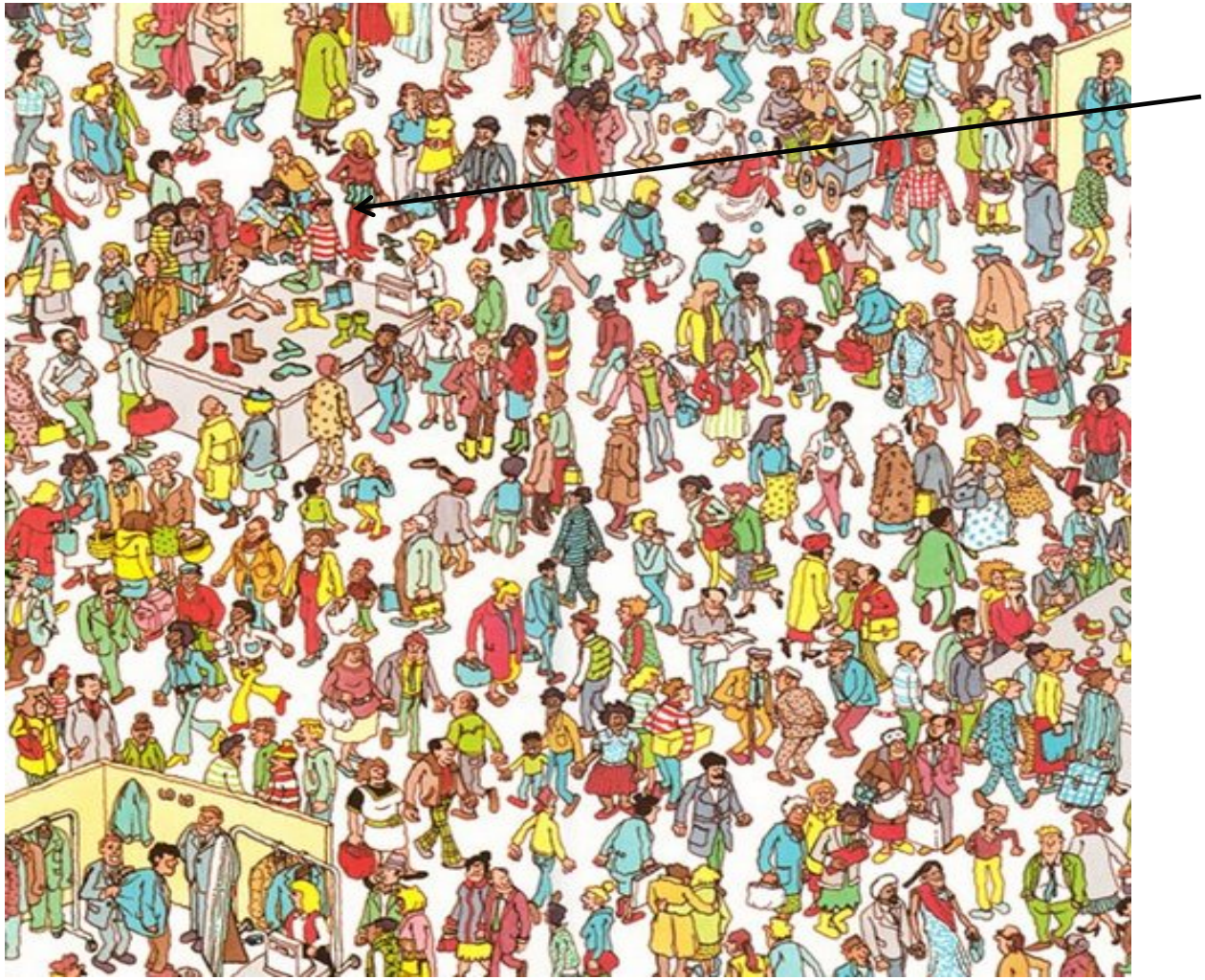
Incident Handlers

Mandiant

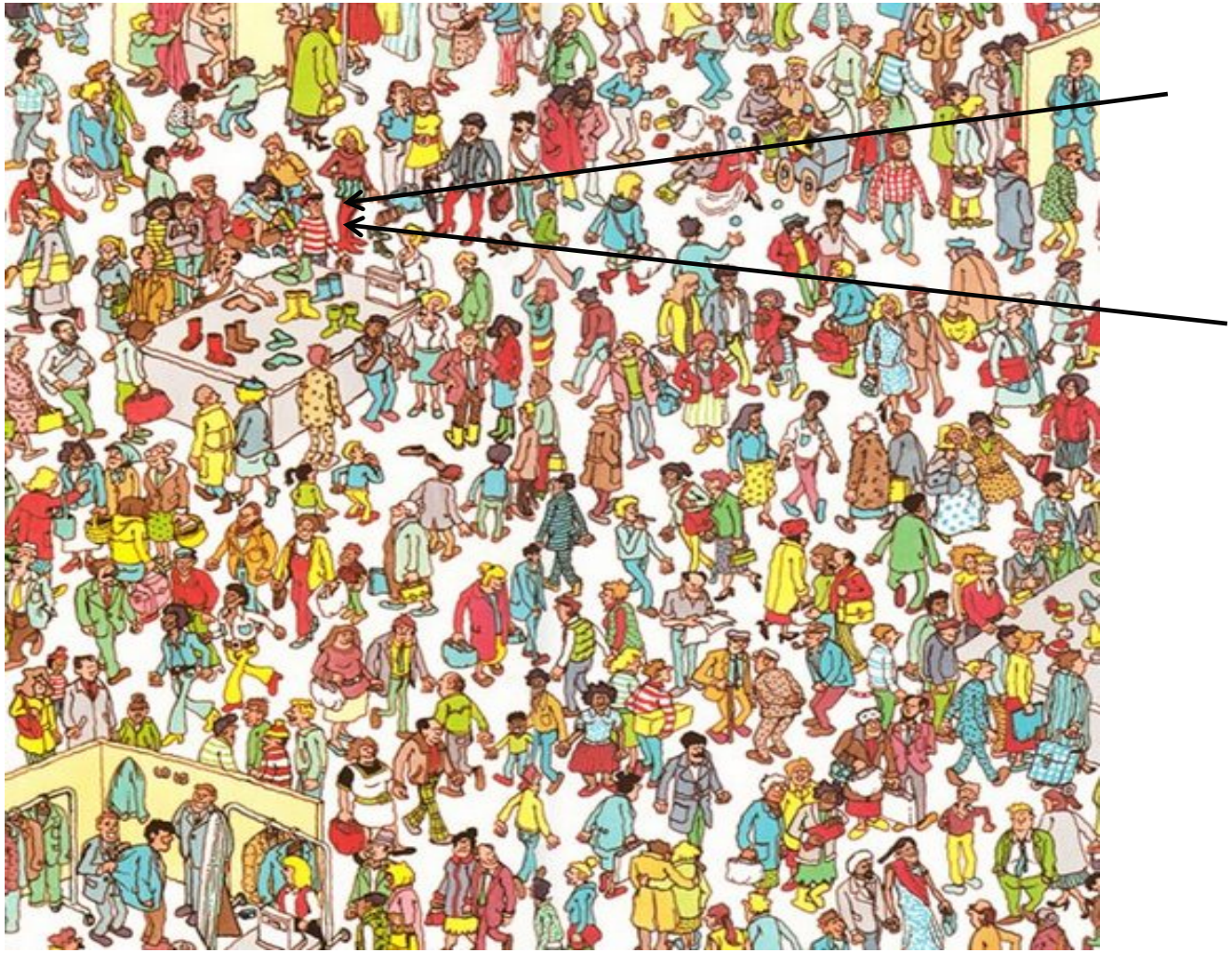
Our Mission

MIRcon 2013

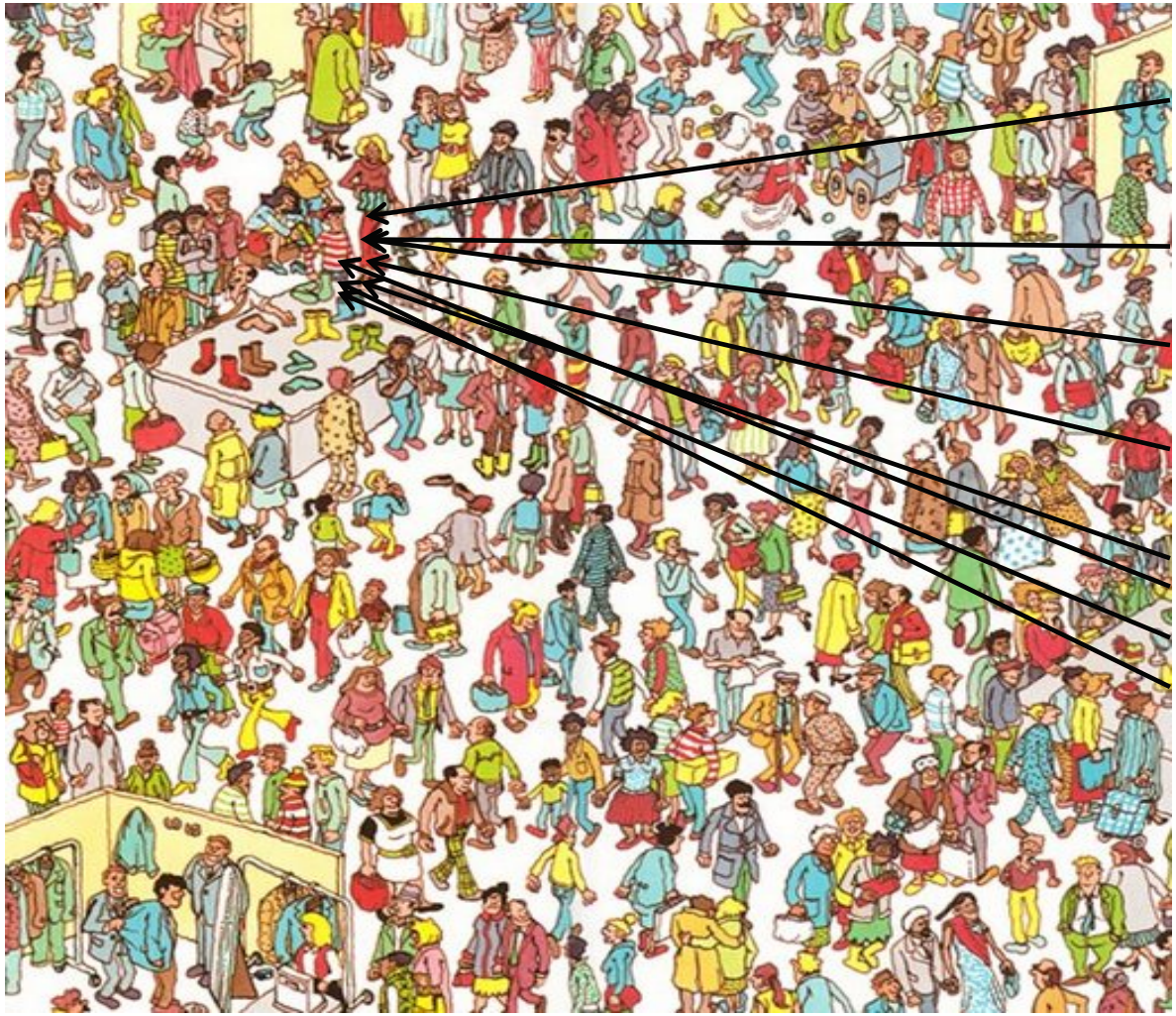
Our Mission



Our Mission



Our Mission



Waldo is evil. We find Waldo.

The First Alert

Three Questions

- How Are They Communicating?
- How Did They Get In?
- Where Are They Going Next?

How Are They Communicating?

Quick Data

- Process Memory
  - Full Listing
  - Command Line History
- Network Data
  - Ports Listing
  - DNS Cache
- Persistence

Process Listing

Process	PID	CPU	Private Bytes	Working Set	Command Line
vmacthlp.exe	908		612 K	2,504 K	"C:\Program Files\VMware\VMware Tools\vmacthlp
svchost.exe	924		3,052 K	4,992 K	C:\WINDOWS\system32\svchost -k DcomLaunch
wmiprvse.exe	3384		2,448 K	4,960 K	C:\WINDOWS\system32\wbem\wmiprvse.exe
svchost.exe	1008		1,892 K	4,548 K	C:\WINDOWS\system32\svchost -k rpcss
SbieSvc.exe	1044		1,064 K	2,600 K	"C:\Program Files\Sandboxie\SbieSvc.exe"
svchost.exe	1116		14,860 K	24,968 K	C:\WINDOWS\system32\svchost.exe -k netsvcs
svchost.exe	1200		1,408 K	3,748 K	C:\WINDOWS\system32\svchost.exe -k NetworkS
svchost.exe	1240		1,668 K	4,148 K	C:\WINDOWS\system32\svchost.exe -k LocalServ
spoolsv.exe	1332		3,780 K	5,780 K	C:\WINDOWS\system32\spoolsv.exe
svchost.exe	1408		1,304 K	3,756 K	C:\WINDOWS\system32\svchost.exe -k LocalServ
jqs.exe	1496		2,168 K	1,404 K	"C:\Program Files\Java\jre6\bin\jqs.exe" -service -c
vmtoolsd.exe	1564		7,724 K	10,020 K	"C:\Program Files\VMware\VMware Tools\vmtoolsc
VMUpgradeHel...	1648		1,016 K	4,104 K	"C:\Program Files\VMware\VMware Tools\VMUpgr
alg.exe	1952		1,160 K	3,628 K	C:\WINDOWS\System32\alg.exe
svchost.exe	2184		2,404 K	4,324 K	C:\WINDOWS\system32\svchost.exe -k imgsvc
lsass.exe	756		3,820 K	1,608 K	C:\WINDOWS\system32\lsass.exe
explorer.exe	3832		12,500 K	17,128 K	C:\WINDOWS\explorer.exe
VMwareUser.exe	856		5,680 K	9,720 K	"C:\Program Files\VMware\VMware Tools\VMware
notepad.exe	540		964 K	468 K	"C:\WINDOWS\System32\NOTEPAD.EXE" C:\Do
procexp.exe	3004		9,584 K	13,312 K	"C:\Sysinternals\procexp.exe"
cmd.exe	460		2,008 K	2,724 K	"C:\WINDOWS\system32\cmd.exe"
explorer.exe	2224		9,552 K	5,512 K	"C:\WINDOWS\explorer.exe" /e,::{20D04FE0-3AE
SandboxieRpcSs.exe	3220		1,956 K	3,600 K	"C:\Program Files\Sandboxie\SandboxieRpcSs.exe
SandboxieDcomLaunch....	2100		1,656 K	2,932 K	"C:\Program Files\Sandboxie\SandboxieDcomLaun
FakeNet.exe	3660		6,252 K	1,600 K	"C:\Documents and Settings\user\Desktop\FakeN
ipconfig.exe	4032		68 K	52 K	
svchost.exe	3160		5,596 K	8,400 K	C:\WINDOWS\system32\svchost.exe 201 0
msiexec.exe	3652	3.08	1,504 K	3,224 K	C:\WINDOWS\system32\msiexec.exe 209 3160

Command Line History

- CSRSS or Conhost Strings

```
\WINDOWS\system32\CMD.EXE - whoami
\WINDOWS\system32\CMD.EXE - "c:\windows\temp\gs.exe > c:\windows\temp\gs.txt"
\WINDOWS\system32\CMD.EXE - ping -n 1 fileserv.acmeco
\WINDOWS\system32\CMD.EXE - net use \\fileserv M1keR0cks! /user:Mike@acmeco
\WINDOWS\system32\CMD.EXE - copy gs.exe \\10.199.5.19\c$\windows\temp\a.exe
\WINDOWS\system32\CMD.EXE - net time \\fileserv
\WINDOWS\system32\CMD.EXE - at \\fileserv 16:45 cmd /c "c:\windows\temp\a.exe > c:\windows\temp\a.txt"
\WINDOWS\system32\CMD.EXE - dir \\fileserv\c$\windows\temo\windows\
\WINDOWS\system32\CMD.EXE - dir \\fileserv\c$\windows\temp\windows\
\WINDOWS\system32\CMD.EXE - at \\fileserv 1 /d
```

Ports Listing

Active Connections

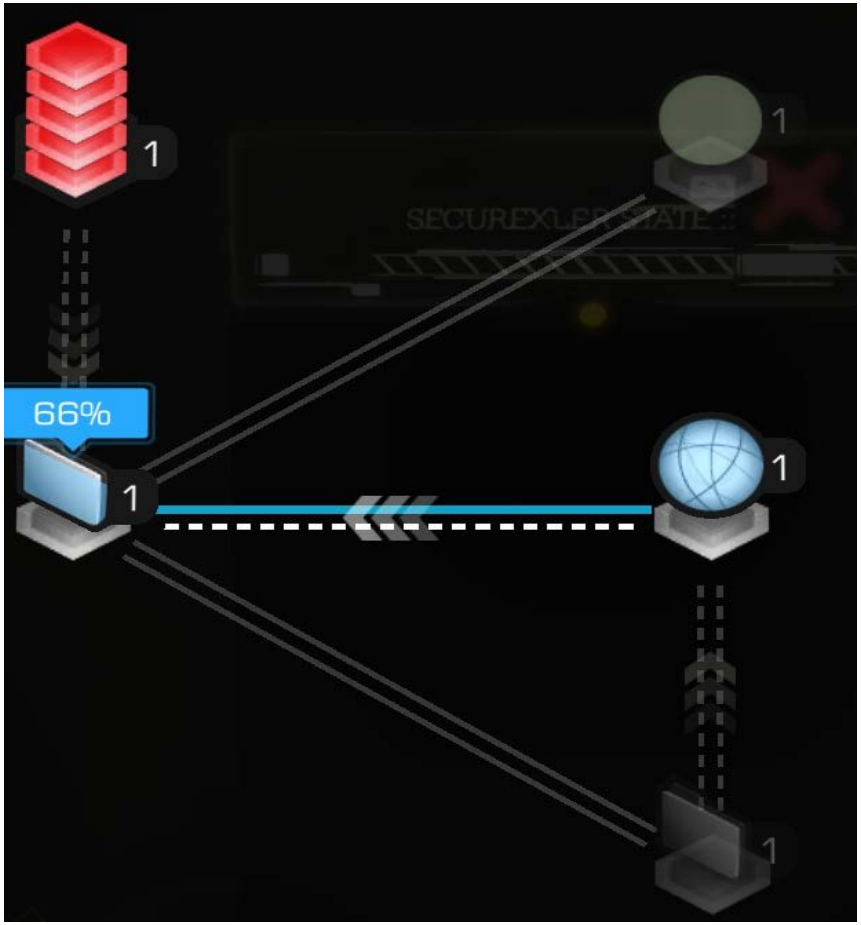
Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:25	0.0.0.0:0	LISTENING	3660
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING	3660
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	1008
TCP	0.0.0.0:443	0.0.0.0:0	LISTENING	3660
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:8080	0.0.0.0:0	LISTENING	3660
TCP	0.0.0.0:8443	0.0.0.0:0	LISTENING	3660
TCP	169.254.150.226:139	0.0.0.0:0	LISTENING	4
TCP	127.0.0.1:5152	111.111.111.111:443	ESTABLISHED	3652
TCP	172.20.240.126:53669	192.168.213.8:443	ESTABLISHED	5580

DNS Cache

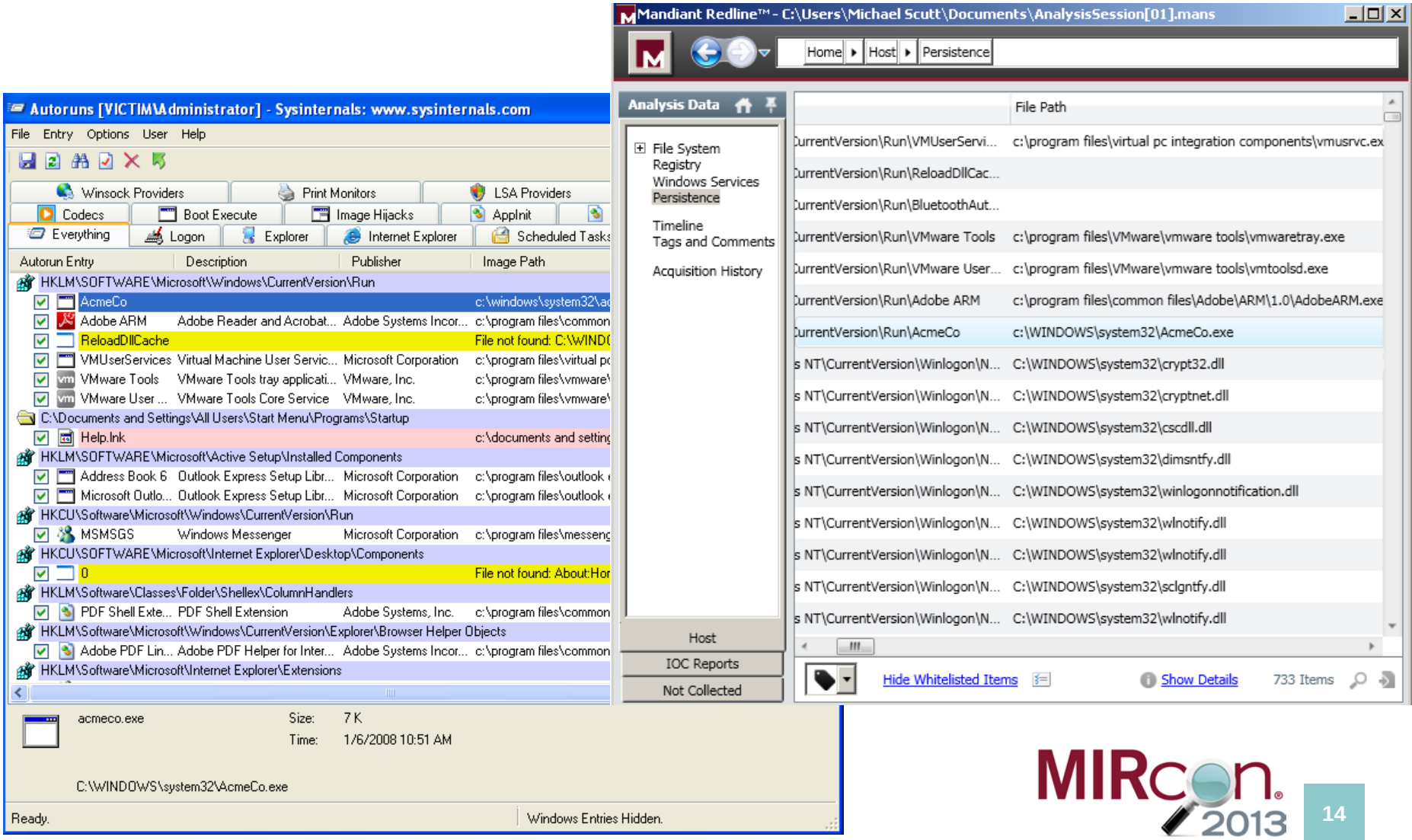
```
badguy.evil.net
----------------------------------------
Record Name . . . . . : badguy.evil.net
Record Type . . . . . : 1
Time To Live  . . . . : 86226
Data Length . . . . . : 4
Section . . . . . . . : Answer
A (Host) Record . . . : 111.111.111.111

feedproxy.google.com
----------------------------------------
Record Name . . . . . : feedproxy.google.com
Record Type . . . . . : 5
Time To Live  . . . . : 88
Data Length . . . . . : 8
Section . . . . . . . : Answer
CNAME Record  . . . . : www4.l.google.com

exchange.acmeco.com
----------------------------------------
Record Name . . . . . : exchange.acmeco.com
Record Type . . . . . : 5
Time To Live  . . . . : 88
Data Length . . . . . : 8
Section . . . . . . . : Answer
CNAME Record  . . . . : 192.168.213.8
```



Persistence



What Does It Mean?

- Putting data together:
  - Identified attacker C2 domain / IP
  - Identified attacker malware and persistence
  - We know how the attackers move and what they want
  - Mike is pwn3d ☹

L33t Hax0r

LOL, Hacked AcmeCo today! Great success!

Like · Comment · Share · about an hour ago ·

2 people like this.

Write a comment...

How Did They Get Here?

Digging Through Historical Data

- Quickly Timelining the Filesystem
- Mining the Event Logs and Registry
- Identifying Credentials

Filesystem Clues

Active	Record type	Filename #1	Std Info Creation date	Std Info Modification	Std Info Access date	Std Info Entry date	FN Info Creation date
Active	Folder	/Windows/SoftwareDistribution/Download/Install	10/03/2013 16:22:18	10/03/2013 16:22:18	10/03/2013 16:22:18	10/03/2013 16:22:18	10/03/2013 16:22:18
Inactive	File	/Windows/Temp/gs.exe	10/03/2013 16:22:18	10/01/2013 05:33:22	10/03/2013 16:22:18	10/03/2013 16:22:13	10/03/2013 16:22:18
Active	File	/System Volume Information/{f6bf75a6-26e4-11e3-ae1d-000c298ce0d2}{3808876b-c176-4e48-b7	10/03/2013 16:22:16	10/03/2013 16:22:16	10/03/2013 16:22:16	10/03/2013 16:22:16	10/03/2013 16:22:16
Active	File	/System Volume Information/SPP/OnlineMetadataCache/{d177b0de-048f-47f0-b571-d0a1877e92	10/03/2013 16:22:16	10/03/2013 16:22:16	10/03/2013 16:22:16	10/03/2013 16:22:16	10/03/2013 16:22:16
Active	File	/ProgramData/Microsoft/Windows Defender/Scans/History/Results/Quick/{D0F7EE63-E4FD-4BEF	10/03/2013 16:21:33	10/03/2013 16:21:33	10/03/2013 16:21:33	10/03/2013 16:21:33	10/03/2013 16:21:33
Active	File	/Windows/System32/config/COMPONENTS{016888b8-6c6f-11de-8d1d-001e0bcde3ec}.TxR.1.regt	10/03/2013 16:21:33	10/03/2013 16:21:33	10/03/2013 16:21:33	10/03/2013 16:21:33	10/03/2013 16:21:33
Active	File	/Windows/System32/config/COMPONENTS{016888b8-6c6f-11de-8d1d-001e0bcde3ec}.TxR.2.regt	10/03/2013 16:21:33	10/03/2013 16:21:33	10/03/2013 16:21:33	10/03/2013 16:21:33	10/03/2013 16:21:33
Active	File	/Windows/System32/config/COMPONENTS{016888b8-6c6f-11de-8d1d-001e0bcde3ec}.TxR.blf	10/03/2013 16:21:33	10/03/2013 16:21:33	10/03/2013 16:21:33	10/03/2013 16:21:33	10/03/2013 16:21:33
Active	File	/Windows/System32/config/COMPONENTS{016888b8-6c6f-11de-8d1d-001e0bcde3ec}.TxR.0.regt	10/03/2013 16:21:33	10/03/2013 16:21:33	10/03/2013 16:21:33	10/03/2013 16:21:33	10/03/2013 16:21:33
Active	File	/Users/USER/AppData/Local/Temp/JETCAD5.tmp	10/03/2013 16:21:15	10/03/2013 16:21:15	10/03/2013 16:21:15	10/03/2013 16:21:15	10/03/2013 16:21:15
Inactive	File	/ProgramData/Microsoft/RAC/Temp/sqlC7B9.tmp	10/03/2013 16:21:14	10/03/2013 16:23:16	10/03/2013 16:21:14	10/03/2013 16:23:16	10/03/2013 16:21:14
Active	File	/Windows/System32/AcmeCo.exe	08/29/2010 09:32:41	08/29/2010 09:33:20	08/30/2010 00:51:08	10/03/2013 16:23:16	10/03/2013 16:21:14
Inactive	File	/Windows/SoftwareDistribution/DataStore/Logs/tmp.edb	10/03/2013 16:21:12	10/03/2013 16:21:12	10/03/2013 16:21:12	10/03/2013 16:21:12	10/03/2013 16:21:12
Active	File	/Users/USER/AppData/Local/Temp/MsoSync.exe_c2rdll(2013100316211754).log	10/03/2013 16:21:11	10/03/2013 16:21:11	10/03/2013 16:21:11	10/03/2013 16:21:11	10/03/2013 16:21:11
Active	File	/Windows/System32/PSEXESVC.EXE	10/03/2013 16:21:11	10/03/2013 16:26:33	10/03/2013 16:21:11	10/03/2013 16:26:33	10/03/2013 16:21:11
Active	File	/Windows/SoftwareDistribution/Download/ad4398dfb942ba3d8d5df90d236d49f8067ce585	10/01/2013 05:33:22	10/01/2013 05:33:22	10/01/2013 05:33:22	10/03/2013 16:22:13	10/01/2013 05:33:22
Active	File	/Users/USER/AppData/Local/Microsoft/Office/15.0/OfficeFileCache/LocalCacheFileEditManager/f	09/30/2013 16:28:24	09/30/2013 16:28:24	09/30/2013 16:28:24	09/30/2013 16:28:24	09/30/2013 16:28:24
Active	File	/Users/USER/AppData/Local/Microsoft/Office/15.0/OfficeFileCache/FSD-{DA8FB960-834E-4740-9	09/30/2013 16:28:23	09/30/2013 16:28:24	09/30/2013 16:28:23	09/30/2013 16:28:24	09/30/2013 16:28:23
Active	File	/Users/USER/AppData/Local/Microsoft/Office/15.0/OfficeFileCache/FSD-{D0C3F511-6031-431E-B	09/30/2013 16:28:23	09/30/2013 16:28:23	09/30/2013 16:28:23	09/30/2013 16:28:23	09/30/2013 16:28:23
Active	File	/Users/USER/AppData/Local/Microsoft/OneNote/15.0/OneNoteOfflineCache.onecache	05/21/2013 19:51:41	10/03/2013 16:22:12	09/30/2013 16:13:51	10/03/2013 16:22:12	09/30/2013 16:13:51
Active	Folder	/Users/USER/AppData/Local/Google/Update/Install	09/30/2013 16:06:00	09/30/2013 16:06:00	09/30/2013 16:06:00	09/30/2013 16:06:00	09/30/2013 16:06:00
Active	Folder	/Users/USER/AppData/Roaming/Microsoft/Office/15.0/22009eca/Proofing	09/30/2013 15:26:21	09/30/2013 15:26:21	09/30/2013 15:26:21	09/30/2013 15:26:21	09/30/2013 15:26:21

Event Logs

```
Type :                  Information
Date :                  10/3/2013
Time :                  16:21:11
Event :                 7045
Source :                Service Control Manager
Category : None
User :                  ACMECO\superadmin
Computer : WIN-3KKQ01DMS2I
Description:
A service was installed in the system.

Service Name:  PsExec
Service File Name:  %SystemRoot%\PSEXESVC.EXE
Service Type:  user mode service
Service Start Type:  demand start
Service Account:  LocalSystem
```

```
Type :                          Audit Success
Date :                          10/03/2013
Time :                          16:21:08
Event :                         4624
Source :                        Microsoft-Windows-Security-
Auditing
Category :      Logon
User :                          N/A
Computer :      OWNEDBOX.ACMECO.COM
Description:
An account was successfully logged on.
…
Logon Type:                                     3
New Logon:
                Security ID:                    S-1-5-21-
2990868922-1773544019-572936875-1085
                Account Name:                   superadmmin
                Account Domain:                 ACMECO
…
Network Information:
                Workstation Name:               ANOTHERBOX
                Source Network Address:         10.199.5.19
                Source Port:                    29468
```

Compromised Credentials

- We have a new source system
- And remember these strings?

```
\WINDOWS\system32\CMD.EXE - whoami
\WINDOWS\system32\CMD.EXE - "c:\windows\temp\gs.exe > c:\windows\temp\gs.txt"
\WINDOWS\system32\CMD.EXE - ping -n 1 fileserv.acmeco
\WINDOWS\system32\CMD.EXE - net use \\fileserv M1keR0cks! /user:Mike@acmeco
\WINDOWS\system32\CMD.EXE - copy gs.exe \\10.199.5.19\c$\windows\temp\a.exe
\WINDOWS\system32\CMD.EXE - net time \\fileserv
\WINDOWS\system32\CMD.EXE - at \\fileserv 16:45 cmd /c "c:\windows\temp\a.exe > c:\windows\temp\a.txt"
\WINDOWS\system32\CMD.EXE - dir \\fileserv\c$\windows\temo\windows\
\WINDOWS\system32\CMD.EXE - dir \\fileserv\c$\windows\temp\windows\
\WINDOWS\system32\CMD.EXE - at \\fileserv 1 /d
```

A New Lead

Last Modified	Last Update	Path	File Size	Process Exec Flag	
7/25/08 15:16	7/13/13 23:40	c:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\MmcAspExt.dll	97792	N/A	
7/25/08 15:17	7/1/13 23:18	C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe	53248	N/A	
4/14/08 6:30	7/13/13 23:54	C:\WINDOWS\system32\snmpsnap.dll	182272	N/A	
4/14/08 6:30	7/13/13 23:54	C:\WINDOWS\system32\servdeps.dll	56320	N/A	
9/12/09 10:14	9/17/13 17:36	C:\Program Files\Virtual PC Integration Components\vmusrvc.exe	39216	N/A	
4/14/08 6:30	9/30/13 19:21	C:\WINDOWS\system32\sendmail.dll	54784	N/A	
9/27/13 13:10	9/27/13 13:09	C:\Windows\System32\z.exe	388608	N/A	
4/14/08 6:30	9/25/13 20:55	C:\WINDOWS\system32\mydocs.dll	90624	N/A	
9/19/13 15:52	10/4/13 16:48	C:\Documents and Settings\Administrator\Desktop\Collector\GetLogs.bat	833	N/A	
5/1/12 17:12	9/17/13 17:36	C:\Program Files\VMware\VMware Tools\TPAutoConnSvc.exe	378192	N/A	
9/25/13 21:08	10/4/13 16:48	C:\ProgramData\ACME\AcmeCo.exe	8704	N/A	
6/8/12 23:41	9/17/13 17:36	C:\Program Files\VMware\VMware Tools\vmacthlp.exe	432792	N/A	
6/8/12 23:49	9/17/13 17:36	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe	62616	N/A	
6/8/12 23:49	9/17/13 17:36	C:\Program Files\VMware\VMware Tools\vmwaretray.exe	58520	N/A	
5/1/12 17:12	9/17/13 17:36	C:\Program Files\VMware\VMware Tools\TPAutoConnect.exe	685392	N/A	
4/14/08 6:30	5/15/13 15:32	C:\Program Files\Outlook Express\setup50.exe	73216	N/A	
4/14/08 6:30	10/4/13 12:37	C:\WINDOWS\system32\mycomput.dll	90112	N/A	
4/14/08 6:30	10/4/13 12:37	C:\WINDOWS\system32\ntmsmgr.dll	488448	N/A	

Active	Record type	Filename #1	Std Info Creation date	Std Info Modification	Std Info Access date	Std Info Entry date	FN Info Creation date	FN In
Active	File	/Windows/rescache/rc0009/Segment0.cmf	09/25/2013 21:08:13	09/16/2013 06:06:48	09/25/2013 21:08:13	09/25/2013 21:08:14	09/25/2013 21:08:13	09/2
Active	File	/Windows/rescache/rc0009/ResCache.hit	09/25/2013 21:08:12	09/16/2013 06:05:53	09/25/2013 21:08:12	09/25/2013 21:08:13	09/25/2013 21:08:12	09/2
Active	File	/Windows/rescache/rc0009	09/25/2013 21:08:12	09/30/2013 16:28:23	09/25/2013 21:08:12	09/30/2013 16:28:23	09/25/2013 21:08:12	09/2
Active	File	/ProgramData/Microsoft/Event Viewer/Views/View_5.xml	09/25/2013 21:08:11	09/16/2013 06:04:03	09/25/2013 21:08:11	09/25/2013 21:08:12	09/25/2013 21:08:11	09/2
Active	File	/ProgramData/ACME/AcmeCo.exe	09/25/2013 21:08:11	09/25/2013 21:08:11	10/03/2013 23:30:51	09/25/2013 21:08:11	09/25/2013 21:08:11	09/2
Active	Folder	/ProgramData/ACME	09/25/2013 21:08:10	09/25/2013 21:08:10	10/03/2013 23:30:51	09/25/2013 21:08:11	09/25/2013 21:08:10	09/2
Inactive	File	/Users/USER/AppData/Local/Temp/dropper.exe	09/25/2013 21:08:10	09/25/2013 21:08:10	10/03/2013 23:30:51	09/25/2013 21:08:19	09/25/2013 21:08:10	09/2
Active	File	/ProgramData/Microsoft/Windows/Power Efficiency Diagnostics/energy-report-2013-08-30.xml	09/25/2013 21:08:10	09/25/2013 21:08:21	09/25/2013 21:08:21	09/25/2013 21:08:21	09/25/2013 21:08:10	09/2
Active	File	/Users/USER/AppData/Local/Temp/FireFly(20130830185121578).log	09/25/2013 21:08:10	09/22/2013 19:11:13	09/25/2013 21:08:10	09/25/2013 21:08:10	09/25/2013 21:08:10	09/2
Active	File	/ProgramData/Microsoft/Event Viewer/ExternalLogs/Log_7.xml	09/25/2013 21:08:10	09/25/2013 21:08:21	09/25/2013 21:08:21	09/25/2013 21:08:21	09/25/2013 21:08:10	09/2
Active	File	/Users/USER/AppData/LocalLow/Sun/Java/DeploymentCache/6.0/25/b76ef43-4e1ac72.idx	09/25/2013 21:08:10	09/26/2013 19:42:23	09/25/2013 21:08:10	09/26/2013 19:42:23	09/25/2013 21:08:10	09/2
Active	File	/Users/USER/AppData/LocalLow/Sun/Java/DeploymentCache/6.0/25/b76ef43-4e1ac72	09/24/2013 05:33:31	09/24/2013 05:33:31	09/24/2013 05:33:31	09/25/2013 21:09:22	09/24/2013 05:33:31	09/2
Active	Folder	/Users/USER/AppData/LocalLow/Sun/Java/DeploymentCache/6.0/25	09/12/2013 20:18:44	09/12/2013 20:18:46	09/12/2013 20:18:44	09/12/2013 20:18:46	09/12/2013 20:18:44	09/1
Active	File	/Users/USER/AppData/Local/Google/Chrome/Application/29.0.1547.66/Installer/setup.exe	09/09/2013 15:07:39	09/09/2013 15:06:24	09/09/2013 15:07:39	09/09/2013 15:07:39	09/09/2013 15:07:39	09/0
Active	Folder	/Users/USER/AppData/Local/Google/Chrome/Application/29.0.1547.66/Installer	09/09/2013 15:07:39	09/25/2013 22:08:28	09/25/2013 22:08:28	09/25/2013 22:08:28	09/09/2013 15:07:39	09/0
Active	File	/Users/USER/AppData/Local/Google/Chrome/Application/29.0.1547.66/VisualElements/splash-62	09/09/2013 15:07:39	09/02/2013 18:46:11	09/09/2013 15:07:39	09/09/2013 15:07:39	09/09/2013 15:07:39	09/0
Active	File	/Users/USER/AppData/Local/Google/Chrome/Application/29.0.1547.66/Locales/te.pak	09/09/2013 15:07:39	09/02/2013 18:46:10	09/09/2013 15:07:39	09/09/2013 15:07:39	09/09/2013 15:07:39	09/0
Active	File	/Users/USER/AppData/Local/Google/Chrome/Application/29.0.1547.66/Locales/th.pak	09/09/2013 15:07:39	09/02/2013 18:46:10	09/09/2013 15:07:39	09/09/2013 15:07:39	09/09/2013 15:07:39	09/0

Clues from the Java Cache

```
.....\......t...:.n}P.............
.....:.....................:.........
.....:.....:.....:.....:.....:.....:.....
.....)http
://acmepartnersite.com/news/JavaAp
plet.class....10.253.161.123.....
<null>..HTTP/1.1 200 OK..content-l
ength..110196..last-modified..Mon,
 30 Sept 2013 06:49:22 GMT..conten
t-type..application/octet-stream..
date..Tue, 01 OCT 2013 12:53:56 GM
T..server..Microsoft-IIS/5.0
```

- Applet source in IDX file
- Time to check browsing history

Recap

- Why didn’t we see Patient 0’s Traffic?
- Exploitation vs. Security Gap

Where are they going Next?

The Situation So Far

- We have tools and backdoors
- We have a known earliest time of compromise
- We identified an attack vector

Determining the Stage of the Attack

- Reconnaissance :-|
- Credential Theft :-(
- Lateral Movement :-O
- Data Theft ;_;

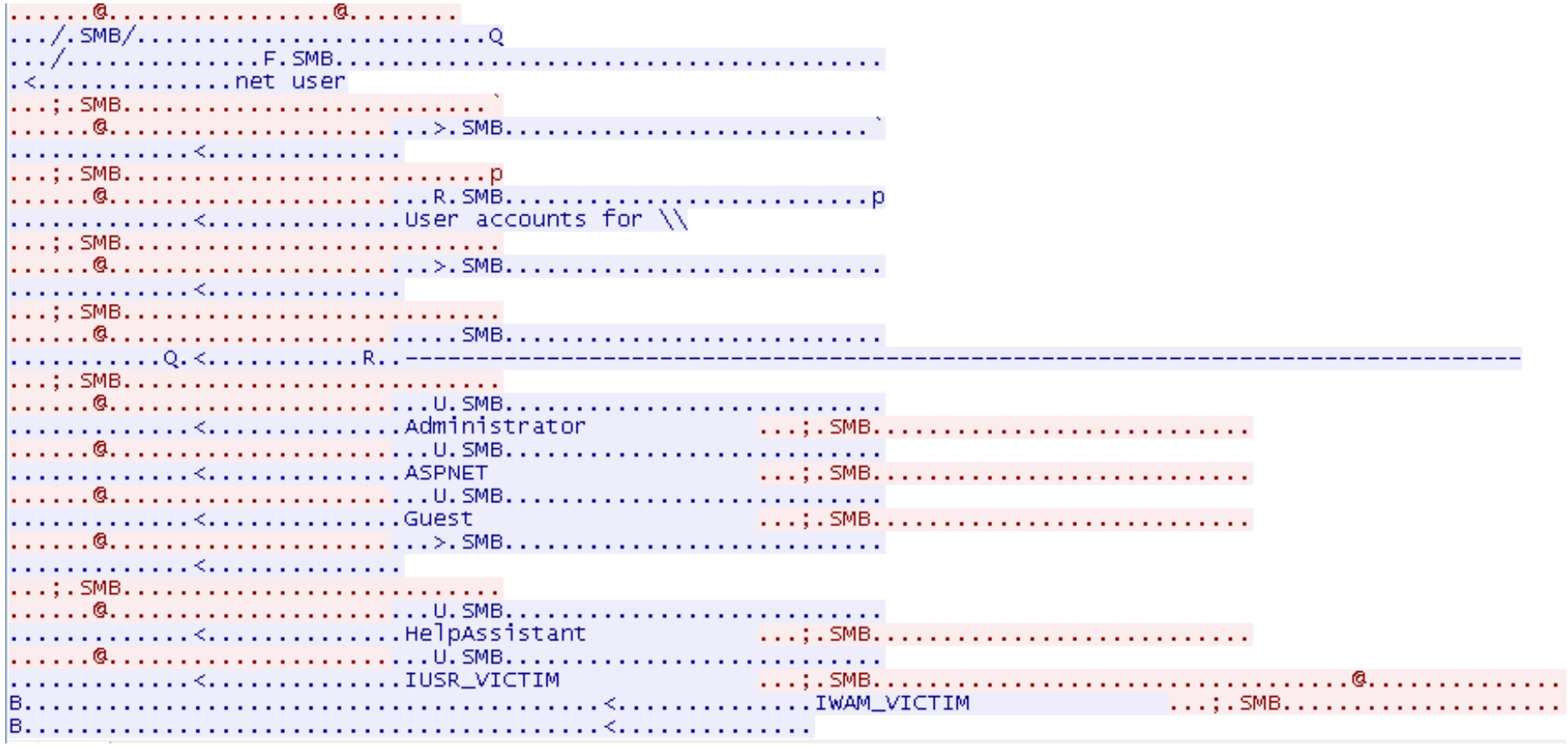
Reconnaissance

Path	Size	File Name	Last Run
C:\WINDOWS\Prefetch\NET.EXE-01A53C2F.pf	17104	NET.EXE	2013-10-04T12:53:15Z
C:\WINDOWS\Prefetch\PING.EXE-28F301A9.pf	13250	PING.EXE	2013-10-04T12:51:49Z
C:\WINDOWS\Prefetch\TASKLIST.EXE-10D94B23.pf	19168	TASKLIST.EXE	2013-10-04T12:51:49Z
C:\WINDOWS\Prefetch\NETSTAT.EXE-2B2B4428.pf	18708	NETSTAT.EXE	2013-10-04T12:51:43Z
C:\WINDOWS\Prefetch\PSEXESVC.EXE-35EFACCF.pf	18676	PSEXESVC.EXE	2013-10-04T12:51:35Z

Credential Harvesting

- Common password theft tools
- Common signs of use

Lateral Movement



Data Theft

- Archives
- Archiving Tools
- Data Transfer Tools

Mission

- Intellectual Property
- Certificates
- Personally Identifiable Information
- Financial Information

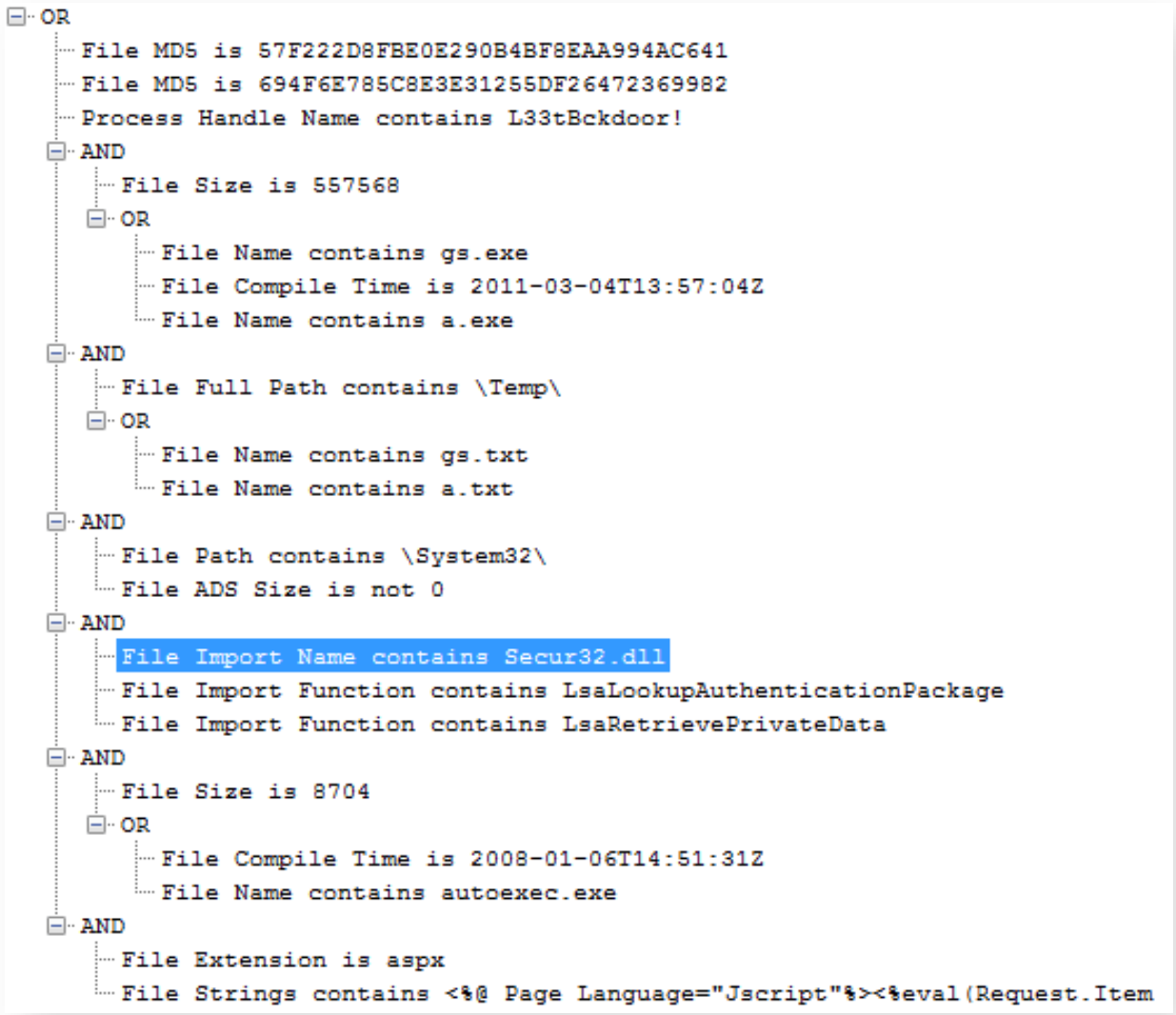
Now What?

READY TO FIND SOME BAD GUYS?
CAN'T WE JUST USE ANTIVIRUS?
imgflip.com

Scoping

- Describe attributes of attacker tools and malware
- Identify forensic artifacts left by attacker activity
- Parse Event Logs for relevant entries
- Collect as much metadata as possible surrounding attacker methodologies

Scoping with Open IOCs



Kick ‘em out

- Block and Sinkhole attacker C2
- Change passwords, lock affected accounts
- Remove compromised hosts
- Secure or shut down ingress systems

Keep ‘em out

- Implement least privilege!
- Application whitelisting
- Network segmentation
- Harden externally visible hosts (this includes code review, SDLC FTW!)
- Implement appropriately restrictive firewall rules (per vlan, trust zone, etc)

Questions?